REMARKS

Claims 1-2, 4-6, 8-16, and 18-29 are all the claims presently pending in the application. It is noted that, notwithstanding any claim amendments made herein, Applicant's intent is to encompass equivalents of all claim elements, even if amended herein or later during prosecution.

Claims 1, 4-7, 10, 15, and 18-20 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Muhme (U.S. Patent No. 5,886,634), further in view of Yeadon (U.S. Patent No. 6,393,339).

Claims 11-14 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Muhme, further in view of Yeadon, and further in view of U.S. Patent No. 4,881,061 to Chambers.

Claims 21-24 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Muhme, further in view of Yeadon, and further in view of U.S. Patent No. 5,883,582 to Bowers et al.

Claims 2 and 16 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Muhme, further in view of Yeadon, further in view of U.S. Patent No. 5,984,388 to Bacon.

Claims 8 and 25 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Muhme, further in view of Yeadon, and further in view of U.S. Patent No. 6,297,727 to Nelson.

Claims 26 and 27 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Muhme, further in view of Yeadon and Nelson, and further in view of US Patent 5,745,036 to Clare.

Claims 9, 28, and 29 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Muhme, further in view of Yeadon, and further in view of US Patent 4,471,343 to Lemelson.

These rejections are respectfully traversed in the following discussion.

I. THE CLAIMED INVENTION

Applicant's invention, as defined, for example, in a non-limiting embodiment of independent claim 1 (and substantially similarly by independent claims 15 and 21) is directed to a system (and method) system for preventing theft of an object.

An electronic article surveillance (EAS) device is operatively attached to an object. A security path, including at least one security gate, detects the EAS device. A reader is operatively

coupled to the security path near one of the security gates. A smart card containing an identification profile of an authorized user is readable by the reader.

A computer attached to the reader disables the security function of the security path at the security gate if a person presenting the smart card at the reader is determined as being authorized to remove said object after having said smart card read by said reader.

With such features, an authorized user of an object in an office environment who exhibits a smart card either does not trigger the alarm or is allowed free passage with the tagged object or the alarm is reset. Or, in an exemplary sales environment, if a retail clerk forgets to remove the EAS device after a legitimate sale, the present invention allows an authorized user, such as a security guard standing near the exit, to reset the alarm by presenting a smart card to the smart card reader located nearby, thereby allowing the alarm to be reset without having to leave the exit area to reset the alarm.

Therefore, the present invention allows a secure method to easily reset a detected security breach that has been activated due to an error. That is, although the card reader might be readily accessible, only a holder of a smart card will be able to reset the system upon activation due to an error. Further, in the office environment, fast reliable tracking of personnel carrying objects (e.g., such as personal computers) into/or of an area can be achieved.

The conventional systems, such as those discussed below and in the Related Art section of the present application, do not have such a structure, and fail to provide for such an operation (e.g., see page 6, lines 18-22 and page 7, lines 1-7 of the present application).

Such features are not taught or suggested by any of the cited references. That is, the present invention includes a new combination of elements such that both a tag attached to an object *and* a smart card are uniquely combined in an unobvious manner to provide features that are not available in the prior art of record, even if the prior art references were properly combinable.

That is, Applicants submit that the present invention is indeed a new combination of elements, particularly since the prior art references do not teach or suggest using a smart card to temporarily disable the security function at a security gate.

II. THE PRIOR ART REJECTIONS

The Examiner alleges that Muhme teaches all elements of claim 1 but concedes that Muhme fails to teach or suggest the use of a smart card. However, as explained in the previous Amendment Under 37 CFR §1.116, filed on February 23, 2004, the rejection currently of record merely walks through various patents that address security and picks components from these references until the Examiner considers that the present invention is thereby redesigned sufficiently to achieve the claimed invention.

Applicants again submit that Judge Rader's holding in *In re Ruiz*, quoted in part in the arguments included in that After Final Amendment, along with the various guidelines recited in the Amendment from the MPEP, as based on case law, clearly demonstrate that this analysis technique is improper.

Applicants maintain their position of the previous argument that the rejection currently of record is improper under the guidelines in the MPEP, based on case law. However, rather than merely recount the previous argument, Applicants additionally submit the following arguments prior to proceeding to appeal.

First, relative to the Examiner's description on page 3 of the Office Action dated April 5, 2004, relative to claim 1, Applicants submit that this description is not what is being claimed.

Applicants are entitled to an analysis based on the plain meaning of the claim language, not on the Examiner's paraphrasing of the prior art reference, in this case, US Patent 5,886,634 to Muhme.

More specifically, in the present invention, as clearly defined by claim 1, the Examiner must find prior art that teaches: "... a smart card for being read by said reader, said smart card containing an identification profile of an authorized user of said object; and a computer attached to said reader, said computer disabling a security function of said security path at said security gate if a person presenting said smart card at said reader is determined as being authorized to remove said object after having said smart card read by said reader."

The Examiner concedes that Muhme fails to teach or suggest the smart card and relies upon Yeadon to overcome this deficiency.

However, before proceeding with commends on the urged modification of Muhme with Yeadon, Applicants submit that Muhme does not teach, suggest, or render obvious the disabling of the security function at a gate, based upon presenting a smart card or, as in the case of Muhme, a second tag. That is, Applicants respectfully submit that the present invention operates in a fundamentally different manner by temporarily disabling the security function at the gate adjacent to the card reader when a smart card having the appropriate identification profile is presented.

In contrast, the fundamental process in Muhme is that of confirming that a second tag is also detected, given the detection of a first tag (e.g., lines 14-16 of column 5). Applicants submit that the Examiner cannot simply ignore this fundamental difference in the process.

At no time is the security function disabled in Muhme. In Muhme, the security function is always enabled. If there is a second tag detected and the database in Muhme determines that the second tag is proper, the security function remains enabled. If there is no second tag detected or the second tag is improper, the security function remains enabled and, indeed, activates the alarm or secures the exit door.

In the present invention, a key concept is that the smart card is used to temporarily disable the security function at the gate associated with the reader. That is, in the present invention, the object-associated tag is continuously emitting its signal. If the sensor in the security gate is temporarily disabled, it will not sense the object-associated tag and set off the alarm. The temporary disablement is achieved by determining that the smart card has been presented by a person whose profile is pre-stored in memory as an authorized user.

In contrast, Muhme does not disable the security function. Rather, it confirms that a second tag has been sensed and that this sensed second tag is the correct second tag, as confirmed by checking the association pre-stored in memory.

This fundamental difference in design of the present invention provides a benefit of flexibility not present in Muhme.

More specifically, if the present invention is used in a retail environment, the smart card aspect allows a secured method to have a local "reset" function. That is, a security attendant or cashier can have a smart card that, upon presentation to the card reader, temporarily disables the security function at that gate, should a cashier forget to remove the tag on the object. Thereby, the smart card serves as a method to reset the alarm in a manner more secure than a simple

RESET switch. Moreover, the physical presence of the card reader near the gate would provide a visible indication of security to the public that may not otherwise be apparent with a simple tag detector.

In the office environment, the temporary disablement aspect of the present invention provides the benefit that the smart card could be an existing employee badge or identification card normally used for entry into the facility. The addition of security for objects, as taught by the present invention to temporarily disable the security function for tagged objects upon presentation of the smart card at the reader, then becomes a low cost method to expand an existing security system to incorporate protection for objects.

Because Muhme is configured to expressly confirm an association with "... an authorized person, an authorized container, or both", as clearly stated at lines 38-39 of column 1, even as modified to incorporate a smart card as used in Yeadon, it does not have the benefit of the flexibility identified above.

First, in the retail environment, because Muhme expressly depends upon confirming the pre-stored association between the tag on the object with at least one other tag, the Examiner cannot simply ignore or modify this feature. At most, the Examiner might want to replace the second tag with the smart card of Muhme.

However, such substitution would only contradict the statement at lines 15-17 of column 1 of Muhme that seemingly discounts the value of card readers, presumably because a card reader would force the user 14 shown in Figures 1 and 2 to stop and swipe the card. Arguably, the key advantage of using two tags, both automatically sensed, is that this configuration eliminates this inconvenience to the user. Moreover, arguably, the whole purpose of Muhme is the elimination of the inconvenience for the user to have to stop and swipe the card. Therefore, Muhme can only be reasonably described as expressly teaching against incorporation of a smart card with a reader.

Because Muhme expressly requires two automatically-sensed tags, in order to reset the alarm in the case in which the object-associated tag is inadvertently left on by the cashier, the person resetting the alarm would still have to have the second tag, in addition to the smart card incorporated from Yeadon, before the alarm could be turned off.

This is because Muhme does not teach or suggest the feature that the second tag be used to disable the security function. Rather, the second tag is used for the entirely different purpose

of confirming a pre-stored association between the first tag and the second tag, thereby determining that the two tags together indicate that the object can be removed without setting off a security condition such as closing a security gate or setting off an alarm.

In contrast, because the smart card in the present invention is used to temporary disable the security function at the gate, it can serve as a mechanism to reset the alarm, should a cashier forget to remove the object-associated tag.

In the office environment, the same disadvantage occurs if Muhme is modified to further incorporate a smart card such as taught in Yeadon. That is, in order to leave with a computer, an employee would have to have possess both the smart card and the second automatically-sensed tag, a clear inconvenience to the employee.

It is also noted, prior to appeal, that even if Muhme were to be modified to incorporate the smart card of Yeadon, the combination would not satisfy the plain meaning of the language of the independent claims. That is, neither Muhme nor Yeadon teaches or suggests the mechanism of disabling the security feature. Therefore, even if Muhme were to be modified to include a smart card, the combination would not satisfy the plain-meaning description in the independent claims.

Furthermore, it is also noted that the smart card of Yeadon is used to gain access to use the dispensing device, either for stocking or for dispensing. This problem of securing the access to a device is quite different from that of the problem of allowing exit through a security gate with a secured object. This difference in problem is exactly the concern of Judge Rader's holding in *In re Ruiz* and is clear evidence of impermissible hindsight in the rejection currently of record.

Moreover, the rejection currently of record fails to describe exactly how Muhme would be modified to incorporate the smart card of Yeadon. The Examiner does state, however, that such modification would "... provide a more secure system". Presumably, therefore, the Examiner intends to simply add the smart card of Yeadon to be a second security method.

As indicated above, such addition would impose a huge burden on the user of Muhme, since the user would have to additionally stop to swipe the smart card.

Therefore, Applicants request that the Examiner, prior to proceeding to appeal, state on the record precisely how the security method of Muhme becomes "more secure" and what exactly is the modification intended to be incorporated into Muhme.

Upon reflection, it is clear that the addition of the smart card into Muhme is much more of a burden than a benefit, thereby again providing clear evidence of impermissible hindsight. That is, any second security system method could be added to Muhme, if "more security" is desired. There is no necessity that the second system be based on a smart card.

Indeed, Applicants suggest that addition of a second security system actually has very little, if any, practical value, particularly considering the added cost of the inconvenience of having to stop to swipe a card. It is clear that the second security system would add value only if the first system (e.g., the one taught in Muhme) should fail.

That is, in order to have additional security value, the only scenario in which the added smart card of Yeadon would add security to the method of Muhme is the scenario in which the smart card provides an alarm indication when the method of Muhme should have provided an alarm but failed to do so. Such added-value indications would occur in only the very-limited situations:

- the second tag is determined by the Muhme computer as being associated with the object-related tag when, in reality, the second tag should have indicated no association (e.g., an error in the database);

- the Muhme sensor fails to detect the object-related first tag, thereby failing altogether to detect the object; and

- the Muhme system has a failure that happens to occur during the period of an unauthorized object removal.

In all of the above scenarios, it is clear that the benefit of any second security system arises only because the Muhme method fails. However, a second system based on a card reader would not be any more attractive than any other second system. For example, Applicants submit that one of ordinary skill in the art would be much more inclined to simply add redundancy into the Muhme method, rather than drastically increasing cost by adding a whole new second system.

Simply picking out the card reader in Yeadon, as done in the rejection of record, is exactly what Judge Rader states as being impermissible, particularly when the problems being addressed by the two prior art references are not precisely the same problem, as discussed above.

Finally, the Examiner relies upon Chambers as demonstrating that a magnetic strip is a known element in the art, upon Bowers as demonstrating that continuous transmission of a tag is

a known element in the art, upon Bacon as demonstrating that an acousto-magnetic tag is a known element in the art, upon Nelson as demonstrating that a video receiver is a known element in the art, and upon Clare as demonstrating that activating a video image after the alarm is turned off is a known element in the art.

Regardless of whether these additional combinations urged by the Examiner are reasonably proper under the above-recited case law and MPEP guidelines, these additional secondary references do not overcome the basic deficiency in the rejection that Muhme would fail to satisfy the plain meaning of the claim language even if modified by Yeadon.

Hence, turning to the clear language of the claims, there is no teaching or suggestion in Muhme of "... a reader operatively coupled to said security path near one of said at least one security gate; a smart card for being read by said reader, said smart card containing an identification profile of an authorized user of said object; and a computer attached to said reader, said computer disabling a security function of said security path at said security gate if a person presenting said smart card at said reader is determined as being authorized to remove said object after having said smart card read by said reader....", as required by independent claim 1. The remaining independent claims contain similar language.

For the reasons stated above, the claimed invention is fully patentable over the cited references.

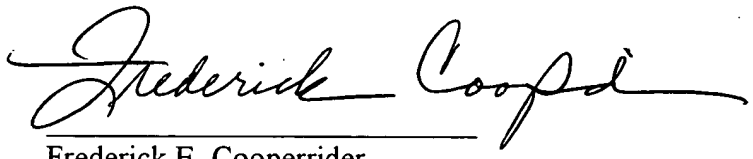
III. FORMAL MATTERS AND CONCLUSION

In view of the foregoing, Applicant submits that claims 1-2, 4-6, 8-16, and 18-29, all the claims presently pending in the application, are patentably distinct over the prior art of record and are in condition for allowance. The Examiner is respectfully requested to pass the above application to issue at the earliest possible time.

Should the Examiner find the application to be other than in condition for allowance, the Examiner is requested to contact the undersigned at the local telephone number listed below to discuss any other changes deemed necessary in a telephonic or personal interview.

The Commissioner is hereby authorized to charge any deficiency in fees or to credit any overpayment in fees to Assignee's Deposit Account No. 50-0510.

Respectfully Submitted,



Frederick E. Cooperrider
Registration No. 36,769

Date: 7/6/04

McGinn & Gibb, PLLC
8321 Old Courthouse Rd. Suite 200
Vienna, VA 22182-3817
(703) 761-4100
Customer No. 21254